AF
IFW

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date set forth below.

by Renee D. East
Date of signature and deposit - January 23, 2007

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Benjamin J. Parker et al	)	Group Art Unit: 2136
	)	
Serial No.: 10/003,816	)	Confirmation No.: 4720
	)	
Filed: 10/25/2001	)	Examiner: Carl G. Colin
	)	
For: Network Security Services Architecture	)	Attorney Docket: 1688(15723)

****

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the final rejection of the Examiner dated September 26, 2006, rejecting claims 1-20.

REAL PARTY IN INTEREST

The real party in interest in the present appeal is Sprint Communications Company L.P., assignee of the entire right, title, and interest in the present application.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

The status of the claims is as follows:

Claims allowed: none.
Claims objected to: none.
Claims rejected: 1-20.
Claims withdrawn: none.

The claims being appealed are: 1-20.

STATUS OF AMENDMENTS

No amendment was filed after final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention addresses the growing complexity of making available various different computer security measures to subscribers of computer networks. The invention achieves a convenient and low cost computer security system by deploying a menu of security tools within a local network that can be selected by a user connected to the network. A network architecture of the invention is structured to provide highly effective and flexible security features while greatly simplifying the user experience.

As defined in claim 1, a private network apparatus for connecting a user to an external internet comprises a plurality of security service pathways each providing a respective combination of security service features (page 6, lines 3-20; see pathways 33-37 in Figure 2). A service selection dashboard allows the user to select from a plurality of security service features for user traffic to and from the user (page 5, lines 18-31; page 9, line 12, to page 10, line 2; see steps 65-68 in Figure 4). A network management server is coupled to the service selection dashboard for storing a subscriber configuration in response to the user selected security service features (page 5, lines 24-34; AAA server 24 in Figure 2). a pass-through router couples the user traffic to the external internet independently of the security service pathways (page 5, line 35, to page 6, line 2; router 25 in Figure 2). A service selection gateway is coupled to the user for directing the user traffic to and from one of the service selection dashboard, the pass-through router, or one of the security service pathways (page 5, lines 16-23; concentrator 20 in Figure 2). A security service router couples the plurality of security service pathways to the external internet (page 6, lines 15-19; router 32 in Figure 2). The service selection gateway directs user traffic to the service selection dashboard if the subscriber configuration is in an initialized state (page 5, lines 27-29; steps 52-56 in Figure 3). The service selection gateway directs user traffic to a respective one of the security service pathways or to the pass-through router in response to the subscriber configuration after initialization by the service selection dashboard (page 10, lines 8-20; steps 57-61 in Figure 3).

Claim 14 recites a method of providing security service in a network interface to an external internet comprising the step of directing a user to a captive portal (page 9, lines 15-19; steps 52-53 in Figure 3). Security service features are presented to user (page 9, lines 28-34). A subscription profile is stored for the user in response to security service features selected by the user through the captive portal (page 9, line 37, to page 10, line 6; step 56 in Figure 3). User traffic is received from the user destined for the external internet at a service selection gateway, and then it is determined from the subscription profile which security service features to apply to the user traffic (page 10, lines 8-11; steps 51, 57, and 60 in Figure 3). If the subscription profile for the user includes any security service features, then the user traffic is re-directed to a particular security service pathway of a plurality of security service pathways, the particular security service pathway corresponding to the security service features identified by the user profile (page 10, lines 14-20; steps 60 and 61 in Figure 3). If the subscription profile for the user includes no security service features, then the user traffic is re-directed to a pass-through router for coupling the user traffic to the external internet (page 10, lines 11-14; step 58 in Figure 3).

None of the claims contain either a means plus function or a step plus function element.

GROUNDS OF REJECTION TO BE REVIEWED

1. Whether Claims 1, 2, 4, 5, 9-14, and 16-20 are unpatentable under 35 U.S.C. §103(a) over Wadlow et al in view of Barrett.

ARGUMENT

Rejection of Claim 1 under 35 USC 103(a); Wadlow in View of Barrett

Claim 1 recites a network architecture wherein a plurality of security service pathways each provide a respective combination of security service features. A service selection gateway directs user traffic to a respective one of the security service pathways or to a pass-through router in response to a subscriber configuration. Consequently, a highly efficient handling of user traffic is obtained because once particular packets are sent to a security service pathway the corresponding combination of security features are automatically applied to the packets, unlike the prior art which requires routing decisions for each packet to be made at each security element in order to send it to the next security element in a combination.

Wadlow fails to disclose security service pathways wherein each pathway provides a respective combination of security service features. Figure 4 of Wadlow shows the various points where different types of packet filtering can be performed. Figure 6 shows various points where different types of application filtering can be performed. Any particular traffic is routed among the necessary points depending upon the desired security for a user. For example, Figure 7 of Wadlow shows a multi-element path for providing a directly-routed, packet-filtered path passing through points Pcsr-cpn, Pcsr-ctc, Pclr-ctc, Pclr-psn, Per-psn, and Per-in. Figure 8 shows a multi-element path to provide an application-filtered connection (i.e., a different combination of security features), wherein the corresponding packets are still routed to packet-filtering points Pcsr-cpn, Pcsr-ctc, Pclr-ctc, Pclr-psn, Per-psn, and Per-in and are additionally routed to application-filtering point Ahag-psn. Therefore, Wadlow fails to teach or suggest the plurality of security service pathways of the present claims which each provide a respective combination of security service features. Upon being directed to a pathway by the service selection gateway, no further routing between security devices is necessary with the present invention since the pathway defines the security features. In contrast, Wadlow consumes resources to decide whether a packet leaving point Per-in in the above example should next go to point Ahag-psn or to a different point.

The distribution of packets by the present invention to the correct security service pathway having the desired combination of security service features depends upon the service selection gateway identifying the appropriate pathway and then routing a packet to the entry point of that pathway. From then on, the packet automatically passes through the selected security features. The architecture in Wadlow is incapable of performing in this claimed manner.

The addition of Barrett fails to strengthen the rejection. Barrett merely shows that a device through which all traffic is passing can be reconfigured to provide different levels of security. It provides no motivation or suggestion to reconstruct a different network architecture so that there are a plurality of security service pathways each providing a respective combination of security service features and a service selection gateway distributing packets to a particular pathway based on a subscriber configuration.

In the Response to Amendment section of the final rejection, it is argued that the feature of the security service pathways that once traffic is directed to a pathway no further routing between security devices is not necessary is not recited. Appellant respectfully disagrees. It is recited that each security service pathway provides a respective combination of security service features, that the service selection gateway directs user traffic to and from one of the security service pathways, and that the security service router couples the plurality of security service pathways to the external internet. Thus, each pathway is distinct from the other pathways and each is separately coupled to the external internet through the security service router. Therefore, the suggestion in the final rejection that Appellant relies on unrecited features is erroneous. Thus, claim 1 and its dependent claims 2, 4, 5, and 9-13 are allowable over the cited references and the rejection should be reversed.

Rejection of Claim 14 under 35 USC 103(a); Wadlow in View of Barrett

Claim 14 recites a method of providing security service in a network interface to an external internet comprising the step of directing a user to a captive portal. Security service features are presented to user. A subscription profile is stored for the user in response to security service features selected by the user through the captive portal. User traffic is received from the user destined for the external internet at a service selection gateway, and then it is determined from the subscription profile which security service features to apply to the user traffic. If the subscription profile for the user includes any security service features, then the user traffic is re-directed to a particular security service pathway of a plurality of security service pathways, the particular security service pathway corresponding to the security service features identified by the user profile. If the subscription profile for the user includes no security service features, then the user traffic is re-directed to a pass-through router for coupling the user traffic to the external internet. Consequently, a highly efficient handling of user traffic is obtained because once particular packets are sent to a security service pathway the corresponding combination of security features are automatically applied to the packets, unlike the prior art which requires routing decisions for each packet to be made at each security element in order to send it to the next security element in a combination.

As explained above regarding claim 1, Wadlow fails to disclose security service pathways wherein each pathway provides a respective combination of security service features. Figure 4 of Wadlow shows the various points where different types of packet filtering can be performed. Figure 6 shows various points where different types of application filtering can be performed. Any particular traffic is routed among the necessary points depending upon the desired security for a user. For example, Figure 7 of Wadlow shows a multi-element path for providing a directly-routed, packet-filtered path passing through points Pcsr-cpn, Pcsr-ctc, Pclr-ctc, Pclr-psn, Per-psn, and Per-in. Figure 8 shows a multi-element path to provide an application-filtered connection (i.e., a different combination of security features), wherein the corresponding packets are still routed to packet-filtering points Pcsr-cpn, Pcsr-ctc, Pclr-ctc, Pclr-psn, Per-psn, and Per-in and are additionally routed to application-filtering point Ahag-psn. Therefore, Wadlow fails to teach or suggest the plurality of security service pathways of the present claims which each provide a respective combination of security service features. Upon being directed to a pathway by the service selection gateway, no further routing between security devices is necessary with the present invention since the pathway defines the security features. In contrast, Wadlow consumes resources to decide whether a packet leaving point Per-in in the above example should next go to point Ahag-psn or to a different point.

The distribution of packets by the present invention to the correct security service pathway having the desired combination of security service features depends upon the service selection gateway identifying the appropriate pathway and then routing a packet to the entry point of that pathway. From then on, the packet automatically passes through the selected security features. The architecture in Wadlow is incapable of performing in this claimed manner.

The addition of Barrett fails to strengthen the rejection. Barrett merely shows that a device through which all traffic is passing can be reconfigured to provide different levels of security. It provides no motivation or suggestion to reconstruct a different network architecture so that there are a plurality of security service pathways each providing a respective combination of security service features and a service selection gateway distributing packets to a particular pathway based on a subscriber configuration. Neither Barrett nor Wadlow disclose or suggest user traffic being re-directed to a particular security service pathway of a plurality of security service pathways, the particular security service pathway corresponding to the security service features identified by the user profile. Moreover, Barrett neither teaches nor suggests creating a user profile of security service features where that combination of service features is obtained by directing traffic to a corresponding pathway. Thus, claim 14 and its dependent claims 16-20 are allowable over the cited references and the rejection should be reversed.

Claims 3, 6-8, and 15

Claims 3, 6-8, and 15 which were rejected under 35 USC 103(a) as being unpatentable over Wadlow et al in view of Barrett and further in view of Schneider et al are allowable as being dependent upon allowable base claims and, thus, are not specifically addressed herein.

CONCLUSION

The final rejection has failed to establish a case of prima facie obviousness of any of claims 1-20. The prior art relied upon in the final rejection neither teaches nor suggests the structure or function of the present invention nor does it provide any teaching which can obtain the significant advantages which are achieved by the present invention. Accordingly, the rejection contained in the final rejection dated September 26, 2006, should be reversed.

Respectfully submitted,

Mark L. Mollon

Mark L. Mollon
Registration No. 31,123
Attorney for Appellant

Date: January 23, 2007
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fourth Floor
720 Water Street
Toledo, Ohio 43604
Tel: 734-542-0228
Fax: 734-542-9569

CLAIMS APPENDIX

Claims 1-20 now read as follows:

1. Private network apparatus for connecting a user to an external internet comprising:

a plurality of security service pathways each providing a respective combination of security service features;

a service selection dashboard allowing said user to select from a plurality of security service features for user traffic to and from said user;

a network management server coupled to said service selection dashboard for storing a subscriber configuration in response to said user selected security service features;

a pass-through router for coupling said user traffic to said external internet independently of said security service pathways;

a service selection gateway coupled to said user for directing said user traffic to and from one of said service selection dashboard, said pass-through router, or one of said security service pathways; and

a security service router for coupling said plurality of security service pathways to said external internet;

wherein said service selection gateway directs said user traffic to said service selection dashboard if said subscriber configuration is in an initialized state; and

wherein said service selection gateway directs said user traffic to a respective one of said security service pathways or to said pass-through router in response to said subscriber configuration after initialization by said service selection dashboard.

2. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall.

3. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a virus scanner.

4. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter.

5. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a content filter.

6. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a virus scanner.

7. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter and a virus scanner.

8. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall, a content filter, and a virus scanner.

9. The apparatus of claim 1 wherein said security service pathways include at least two pathways having firewalls, said firewalls respectively providing different grades of firewall protection.

10. The apparatus of claim 9 comprising three security service pathways each including a respective firewall, said firewalls including a first firewall providing a high grade firewall protection, a second firewall providing a medium grade firewall protection, and a third firewall providing a low grade firewall protection.

11. The apparatus of claim 10 wherein said low grade firewall protection comprises port blocking for outgoing traffic.

12. The apparatus of claim 10 wherein said medium grade firewall protection comprises port blocking for incoming and outgoing traffic.

13. The apparatus of claim 10 wherein said high grade firewall protection comprises port blocking for outgoing traffic and blocking of all incoming traffic not initiated by said user.

14. A method of providing security service in a network interface to an external internet, said method comprising the steps of:

directing a user to a captive portal;

presenting security service features to said user;

storing a subscription profile for said user in response to security service features selected by said user through said captive portal;

receiving user traffic from said user destined for said external internet at a service selection gateway;

determining from said subscription profile which security service features to apply to said user traffic;

if said subscription profile for said user includes any security service features, then re-directing said user traffic to a particular security service pathway of a plurality of security service pathways, said particular security service pathway corresponding to said security service features identified by said user profile; and if said subscription profile for said user includes no security service features, then re-directing said user traffic to a pass-through router for coupling said user traffic to said external internet.

15. The method of claim 14 wherein said security service features include firewall services, content filtering services, and virus scanning services, and wherein each of said security service pathways corresponds to a combination of said security service features.

16. The method of claim 15 wherein said firewall services comprise selectable grades of firewall protection including a high grade firewall protection, a medium grade firewall protection, and a low grade firewall protection.

17. The method of claim 16 wherein said low grade firewall protection comprises port blocking for outgoing user traffic.

18. The method of claim 16 wherein said medium grade firewall protection comprises port blocking for incoming and outgoing user traffic.

19. The method of claim 16 wherein said high grade firewall protection comprises port blocking for outgoing user traffic and blocking of all incoming traffic not initiated by said user.

20. The apparatus of claim 1 further comprising:

a user-side switch coupling said service selection gateway to said security service pathways; and an internet-side switch coupling said security service pathways to said security service router.

EVIDENCE APPENDIX

No evidence has been submitted under 37 CFR §§1.130, §§1.131, §§1.132, or otherwise.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings and no corresponding decisions rendered.

PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL
For FY 2006

Effective 12/08/2004. Fee pursuant to the Consolidated Appropriations Act. 2005 (H.R. 4818).

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($ 500.00)

Complete if known	
Application Number	10/003,816
Filing Date	10/25/2001
First Named Inventor	Benjamin J. Parker et al
Examiner Name	Carl G. Colin
Art Unit	2136
Attorney Docket No.	1688(15723)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify):________

☒ Deposit Account: Deposit Acct. Number: 21-0765 Deposit Acct. Name: Sprint Communications Company L.P.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below

☒ Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17

☐ Credit any overpayments

☐ Charge fee(s) indicated below, **except the filing fee** to the above-identified deposit

Warning: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fees Paid ($)**
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims ________ - 20 or HP = **Extra Claims** ________ x **Fee ($)** ________ = **Fee Paid ($)** ________

HP = highest number of total claims paid for, if greater than 20

Indep. Claims ________ - 3 or HP = **Extra Claims** ________ X **Fee ($)** ________ = **Fee Paid ($)** ________

HP = highest number of total claims paid for, if greater than 3

Multiple Dependent Claims
Fee($) ________ Fee Paid ($) ________

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ________ - 100 = **Extra Sheets** ________ / 50 = **Number of each additional 50 or fraction thereof** ________ (round up to a whole number) x **Fee ($)** ________ = **Fee Paid ($)** ________

4. OTHER FEE(S)

Non-English Specification, $130 fee (no small entity discount)

Other: 1402 – 500.00 (Brief on Appeal)

SUBMITTED BY (Complete (if applicable))

Name (Print/Type)	Mark L. Mollon	Registration No. (Attorney/Agent)	31,123	Telephone (734) 542-0900
Signature	Mark L Mollon			Date January 23, 2007

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.
This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** If you need assistance in completing the form, call 1-800-PTO-9199 and select Option 2.